



1220 L Street, Northwest  
Washington, DC 20005-4070  
Tel 202-682-8517  
Fax 202-682-8207  
E-Mail [martink@api.org](mailto:martink@api.org)

**Kendra L. Martin, CAE**  
Director - Security Programs

July 31, 2003

Docket Management Facility  
USCG-2003-14792, 14733, 14749, 14732, 14759  
U.S. Department of Transportation  
Room PL- 401  
400 Seventh Street, SW  
Washington, DC 20590-0001

Attn: Docket Clerk:

The American Petroleum Institute (API) is a national trade association whose members are engaged in all facets of the oil and natural gas industry, including exploration and production, transportation (marine and pipeline), marketing, and refining. As such, our member companies have a direct interest in the series of six temporary interim rules published by the U.S. Coast Guard (USCG) on July 1, 2003, to promulgate maritime security requirements mandated by the Maritime Transportation Security Act of 2002 (MTSA) [68 Federal Register 39239 – 39368].

Because of API's previous involvement in commenting on maritime security issues,<sup>1</sup> and because of the significant impact the proposed requirements may have on our industry, API is pleased to provide these comments on the USCG temporary interim rules (TIRs).

API and its members have a long-standing commitment to protecting the energy infrastructure. Since the events of September 11, 2001, this commitment has been strengthened through the enhancement of numerous private initiatives as well as partnerships with federal, state and local authorities. It is in this spirit of cooperation that API stands ready to assist the USCG to further secure our nation's maritime domain and to protect our critical transportation modes ensuring that energy supplies reach the marketplace.

We commend the USCG for reaching a number of reasonable and practical conclusions on certain specific issues contained in the six TIRs. Despite these merits, certain critical provisions of the rulemaking remain unclear to the regulated community and others are potentially impractical. API will elaborate on our key issues of concern in this cover letter—many of which are overarching issues found within several of the TIRs.

---

<sup>1</sup>On February 27, 2003, API provided formal input to the USCG in response to its December 30, 2002 Federal Register notice requesting comments on Maritime Security via a series of stakeholder meetings [67 Federal Register 79741].

### ***Continued Operation While Security Plans are being Reviewed***

In light of the uncertainties regarding USCG manpower and time constraints, API is pleased to see that the USCG has included within three of the TIRs (Vessel Security, Facility Security and Offshore Facility Security) specific regulatory language that states:

(2) The VSP submitted for approval and a current acknowledgement letter from the Commanding Officer, MSC, stating that the Coast Guard is currently reviewing the VSP submitted for approval, and that the vessel may continue to operate so long as the vessel remains in compliance with the submitted plan; (68 Federal Register 39303 at 104.120).<sup>2</sup>

Our interpretation of these provisions is that vessels and facilities will be able to continue to operate beyond July 1, 2004 if a VSP or FSP has been submitted to the appropriate USCG office and the vessel or facility remains in compliance with the plan. However, if we are interpreting these provisions too broadly, we request immediate notification and clarification.

### ***ISPS Applicability and ISPS Part B***

API is concerned that, by the USCG incorporation of language from the International Ship and Port Facility Security Code (ISPS), the USCG is applying prescriptive, non-performance-based requirements on all regulated facilities. We understand that when ISPS Part B was developed, it was intended to serve as guidance. The USCG has gone beyond ISPS, removed any “guidance” language from the code, and now stipulates that these elements in a security program are mandatory. As such, a foreign flag vessel has less stringent requirements to comply with than Offshore Supply Vessels and other vessels and facilities covered by these regulations. API encourages the USCG to remove the prescriptive language and replace it with the language that reflects the original intent of the ISPS Code. Additionally, these TIRs have requirements that are in addition to those found in ISPS Parts A and B, which are also quite prescriptive. We are attaching a side-by-side comparison of certain elements of Part 105 compared to the applicable elements of the ISPS code (Parts A and B) to illustrate the significant prescriptive nature of the rulemaking (see Attachment II) for your reference. We request these prescriptive elements be removed in the Final Rule.

Additionally, in API’s comments to the USCG on February 27, 2003, we strongly supported an approach of allowing the use of industry security standards, recommended practices and guidelines as alternatives to prescriptive regulatory requirements that would be contained in ISPS-type regulations. This recommendation was repeated a number of times by other organizations, associations and industry representatives during the public meetings USCG held in early 2003. However, the USCG chose not to take this approach in the July 1, 2003 TIRs.

As a follow-up to our letter to Admiral Larry Hereth, dated July 14, 2003, API again urges the USCG to review and approve all of the documents we submitted on that date as Alternate Security Programs for vessel security, facility security and offshore petroleum

---

<sup>2</sup> For Facility Security, similar language can be found at 68 Federal Register 39323 - §105.120; and for Offshore Facility Security, similar language can be found at 68 Federal Register 39345 - §106.115.

operations security, as applicable. Many of these vessels and facilities have already implemented the criteria within these documents and have made significant progress in ensuring the safety and security of the petroleum industry and its impact on maritime transportation activities. By USCG approving these documents as soon as possible, you will enable the oil and natural gas industry to address security needs using a performance-based approach, minimizing unnecessary duplication or the requirement to undo the work that has already been completed.

***Application of these Regulations to all Facilities on Waters of the United States***

A concern for API has been the application of security requirements under the MTSA to onshore facilities that pose little risk as maritime terrorist targets or being involved in a transportation security incident due their inland location. In addition, API seeks clarification on the applicability of the temporary interim rule particularly with regard to facilities on waters *inland* from shore.

MTSA defines “facility” as “any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States. The USCG in the temporary interim rule defines *Waters subject to the jurisdiction of the U.S* in reference to “the navigable waters of the U.S., as defined in 46 U.S.C. 2101(17a); the Exclusive Economic Zone (EEZ) in respect to the living and non-living resources therein; and in respect to facilities located on the Outer Continental Shelf of the U.S., the waters superadjacent thereto” (68 Federal Register 39281). Thus, if API understands these provisions correctly, USCG’s jurisdiction extends *outward* to all waters of the territorial sea of the U.S. out to 12 nautical miles from a state’s coastline, plus the 200-mile EEZ. This understanding appears to be consistent with the USCG’s current regulations at 33 CFR § 2.05-25 and with the recent pronouncement of USCG jurisdiction in the Final Rule issued on July 18, 2003, on Territorial Seas, Navigable Waters, and Jurisdiction (68 Fed. Reg. 42595 (Jurisdiction Rule)).

However, with regard to navigable waters and the implication of this term for waters inland from shore, the temporary interim rule is not clear. API seeks clarification as to whether USCG’s definition of navigable waters found in 33 CFR § 2.05-25(a)(i) and confirmed in USCG’s recent jurisdictional rule issued on July 18<sup>th</sup>, applies to the temporary interim rule. The existing definition in 33 CFR § 2.05-25(a)(i) requires that waters are or have been used as highways for substantial interstate or foreign commerce, and thus are “navigable-in-fact.” API requests confirmation in the temporary interim rule that this concept of navigable waters continues to govern.

Furthermore, API believes that the USCG should only be regulating those facilities that pose a high risk of being involved in a transportation security incident. For example, it does not seem reasonable to impose the same FSP requirements on a remote facility in an inland state adjacent to a small creek, not in navigable waters, as a facility located in or near a major port. Our assumption is that the USCG recognizes the distinction between these facilities by its own requirements whereby, according to §105.115, a FSP must be submitted to a cognizant Captain of the Port (COTP) for review and approval. In other words, it is likely some facilities that are significantly inland would have no cognizant

COTP to contact. If we are misinterpreting this approach, we request immediate clarification.

***Protection from Disclosure of Security-Related Information***

Another topic raised with the USCG in our February 27, 2003 submittal was API's concerns regarding the sensitive nature of vessel and facility-specific information. We were particularly concerned how this information would be protected, once provided to the COTP and the newly formed Area Maritime Security (AMS) Committees with their potential for a large number of stakeholders (up to 200 according to the preamble). Therefore, API recommends that the FSA and FSP be "decoupled" with only the FSP being submitted to the COTP or District. The FSA will be maintained on-site and will be available to the COTP or District during an inspection.

While our preference had been that security-related information, particularly the vulnerability assessments and vessel and facility security plans, be treated as "secret" information and not "security sensitive information (SSI)," which would be consistent with Federal Bureau of Investigation (FBI) and Department of Energy (DOE) classifications, we were satisfied with the material being designated as SSI in accordance with 49 CFR part 1520 and the operating protocol determined by the USCG within the Area Maritime Security TIR.

Additionally, API appreciates the flexibility offered to owners and operators of vessels and facilities, which allows for a request to be made of the Commandant or COTP, for higher designation than SSI, for a particular VSP or FSP. We are encouraged by the USCG's recognition that in all cases, material retained by a federal agency must be safeguarded to the appropriate designation.

I thank you for the opportunity to address these important issues as we work together to protect our nation's maritime borders, energy infrastructure, and the safety of the American people. API and its members stand ready to assist the USCG in this and all future efforts. If you have questions regarding the information offered or would like additional assistance, please don't hesitate to contact me at 202-682-8517 or [martink@api.org](mailto:martink@api.org).

Kendra L. Martin, CAE  
Director - Security Programs  
American Petroleum Institute

cc: RADM Larry Hereth, Director of Port Security, US Coast Guard  
Secretary Tom Ridge, US Department of Homeland Security

ATTACHMENT 1

**COMMENTS OF THE AMERICAN PETROLEUM INSTITUTE  
TO THE UNITED STATES COAST GUARD  
ON ITS TEMPORARY INTERIM RULES  
TO PROMULGATE  
THE MARITIME SECURITY REQUIREMENTS  
OF THE MARITIME TRANSPORTATION SECURITY ACT OF 2002**

**[68 Federal Register 39239 – 39368; Published on July 1, 2003]**

**SUBMITTED TO THE UNITED STATES COAST GUARD ON  
JULY 31, 2003**

**Re: National Maritime Security Initiatives**  
**Docket: USCG-2003-14792, Parts 101 and 102**

***I. Subchapter H – Maritime Security***  
***Part 101 – General Provisions***

***Subpart A - General***

**Section 101.120 Alternatives**

➤ (b) Alternative Security Programs

In API's comments to the USCG on February 27, 2003, we strongly supported the approach of allowing the use of industry security standards, recommended practices and guidelines as alternatives to prescriptive regulatory requirements that would be contained in ISPS-type regulations. This recommendation was repeated a number of times by other organizations, associations and industry representatives during the public meetings USCG held during January and February 2003. However, the USCG chose not to take this approach in the July 1, 2003 IFR.

As a follow-up to our letter to Admiral Larry Hereth, dated July 14, 2003, API again urges the USCG to review and approve all of the documents we submitted on that date as Alternate Security Programs for vessel security, facility security and off-shore petroleum operations security, as applicable. Many of these vessels and facilities have already begun to implement the criteria within these documents and have made significant progress in ensuring the safety and security of the petroleum industry and its impact on maritime transportation activities. By USCG approving these documents as soon as possible, you will enable the oil and natural gas industry to address security needs using a performance-based approach, minimizing unnecessary duplication or the requirement to undo the work that has already been completed.

***Subpart D – Control Measures for Security***

**Section 101.405 Maritime Security (MARSEC) Directive**

➤ (a)(2) This section states that the Coast Guard will publish a notice in the Federal Register, and all affected owners and operators will need to go to their local COTP or cognizant District Commander to acquire a copy of the MARSEC Directive after proving that they are a "covered person," and have a "need to know."

We believe that the stated method of communicating a Directive is cumbersome and unworkable because of the time and effort it would require for the owner or operator to take notice of the MARSEC Directive notice in the Federal Register, gain the proper clearance to receive the Directive, receive the Directive, and finally implement the requirements of the Directive, including any notices to vessels within 96 hours.

We believe that the COTP or cognizant District Commander should provide notice more expeditiously to owners or operators who are covered persons and have a need to know. We suggest adding language in the regulation that would require the COTP or cognizant District Commander to promptly communicate the MARSEC Directive to the affected owners or operators by means in addition to the Federal Register to ensure timely notice and facilitate compliance.

#### Section 101.510 Assessment Tools

- This section lists various assessment methodologies currently recognized by the USCG. API suggests that the USCG include flexible wording in this section to allow acceptance of other assessment methodologies, including those developed by industry, by revising the second sentence to read: “These tools include, but are not limited to, .....”
- For example, API and NPRA recently published the “Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries.” This document was developed by API and NPRA, in close cooperation with the DHS and DOE’s Argonne Laboratory and included pilot testing at industry facilities. Similarly, Appendix E of *API RP 70* has an assessment methodology for exploration and production facilities. As requested earlier in these comments, API encourages the USCG to approve these SVA methodologies as alternatives to the prescriptive language in the temporary interim rule.

**Re: National Maritime Security Initiatives**  
**Docket: USCG-2003-14733, Part 103**

***II. Subchapter H – Maritime Security***  
***Part 103 – Area Maritime Security***

***Subpart C – Area Maritime Security (AMS) Committee***

**Section 103.300 Area Maritime Security (AMS) Committee**

- This section establishes Area Maritime Security (AMS) Committees. API strongly endorses such a concept for oil and natural gas facilities and their support infrastructure for the Gulf of Mexico Outer Continental Shelf as set forth in these interim rules. We urge the USCG to expeditiously commence the AMS process for the Gulf of Mexico OCS.

**Section 103.305 Composition of an Area Maritime Security (AMS) Committee**

- (a) To ensure appropriate membership on these committees, API suggests that the criteria be revised in 103.305(a) to require “at least 5 years of experience related to maritime or port operations” and not necessarily limit the experience requirement to only security-related experience.
- 
- (a)(7) This provision allows port stakeholders affected by security practices or policies to be members of the AMS Committee and, as stated in the preamble, could have as many as 200 representatives. API is very concerned that it will be difficult to protect vessel and facility security information when dealing with groups of stakeholders so large. API strongly urges the USCG to take all steps necessary to protect such information including ensuring that the stakeholders have at least 5 years of experience related to maritime, port operations or offshore oil and natural gas drilling AND that the COTP exercise his/her power to require a security background examination of candidate members before they are placed on the AMS Committee.

**Re: National Maritime Security Initiatives**  
**Docket: USCG-2003-14749, Part 104**

***III. Subchapter H – Maritime Security***  
***Part 104 – Vessel Security***

***Subpart A - General***

Section 104.145 Maritime Security (MARSEC) Directive

- Vessel owner or operators are required to comply with instructions contained in a MARSEC directive under §101.405. These directives announce additional security measures necessary to respond to a particular maritime threat, as determined by the Commandant or his/her delegee. API seeks clarification from the USCG on those that might be considered delegees.
- Obtaining copies of such directives, once the availability of the directives is announced by the USCG, is the responsibility of the owner or operator, as is acknowledgement of its receipt and specifying the measures by which the directive will be implemented. For many of our members, as owners or operators (or with designated Company Security Officers) in foreign ports, these provisions require further clarification. In such cases, we recommend that the USCG consider other “domestic” company designees who would be acceptable recipients of this vital information. For facilities, obtaining copies in person from the local COTP may be possible but, with 45 COTPs, this could be a major exercise for a shipping company CSO. API suggests a secure website/fax/email system be available as an option to obtain the directives.

Section 104.235 Vessel Recordkeeping Requirements

- (7) Under this subsection, the USCG requires that manned vessels keep on board copies of the last 10 Declarations of Security (DoS) and each continuing DoS for at least 90 days. For our members, this is somewhat disconcerting. It takes approximately 45 days for a very large crude carrier (VLCC) to move from a Middle East port to the Louisiana Offshore Oil Platform (LOOP) – and almost three months for a round trip. We are hopeful that the USCG will recognize that such a vessel may take well over a year to collect the 10 declarations required to be maintained on board. The pace by which a vessel attains its series of declarations should not automatically translate into questionable activity or lack of compliance on the part of the vessel, nor should it require additional security measures be imposed on the vessel; it is simply a fact of this particular transportation mode.

Section 104.250 Procedures for Interfacing with Facilities and Other Vessels

- For each U.S. flag vessel that calls in foreign ports or facilities, the vessel owner or operator must ensure procedures for interfacing with those ports and facilities. API’s assumption is that these foreign ports and facilities will accept the compliance documentation addressed in Section 104.120, including an approval letter from the Commanding Officer MSC, stating that the USCG is currently reviewing the VSP, as acceptable in order to “ensure” procedures for a secure vessel/facility interface.

Secondly, assessments will need to be made in order for foreign ports to achieve approved status. This may include assessing hundreds of ports worldwide. Such a tremendous undertaking cannot occur overnight and yet U.S. vessels will be calling on these ports all the while (and vice versa) between July 1, 2003 and July 2, 2004. We request that the USCG be flexible in its application of many of these requirements, as this monumental set of new security procedures unfolds.

#### Section 104.255 Declaration of Security

- This section addresses Declaration of Security (DoS) requirements as a means for ensuring that critical security concerns are properly addressed at the vessel-facility interface prior to any transfer operation. The USCG suggests that the DoS requirement is similar to the existing U.S. practice for vessel-to-facility interface for oil transfer proceedings.

While this requirement appears to be reasonable in its approach, there are a number of uncertainties associated with its application. For example, if a vessel is at one MARSEC level and enters a port and approaches a transfer facility that is at a higher MARSEC level, it appears to be up to the FSO and VSO to coordinate security needs – but in what timeframe? Within 12 hours of the notification? Likewise, where is the vessel located while the details of the DoS are being addressed and to whom is the DoS submitted?

Overall, the numerous unknowns regarding the vessel and facility interface are of particular importance to the oil and natural gas industry. If the USCG intends for the industry to complete a DoS each time a vessel is handed off to another vessel or a facility, the ramifications are significant. We question whether the enhancements to security are as markedly significant. As an industry, we simply have no clear understanding of the true economic and operational impacts imposed by these requirements and will not have such an understanding until the VSPs are actually approved, implemented, and the procedures are underway. API is hopeful that the USCG will be willing to discuss and amend various elements of the requirements, should they simply prove to be too burdensome for the vessel or facility owner or operator.

**Re: National Maritime Security Initiatives**  
**Docket: USCG-2003-14732, Part 105**

***IV. Subchapter H – Maritime Security***  
***Part 105 – Facility Security***

***Subpart A – General***

**Section 105.105 Applicability**

- (a)(1) States that this TIR applies to facilities subject to 33 CFR Parts 126, 127 and 154. In particular, Part 154 applies to facilities capable of transferring oil or hazardous materials, in bulk, to or from a vessel where the vessel has a total capacity of 250 barrels or more. Therefore, it is API's interpretation that facilities that do not transfer oil or hazardous materials from vessels with capacities of 250 barrels or more are not subject to Part 105 of these regulations unless that facility is covered by Parts 126 or 127 or any other requirements in Section 105.105(a).
- API requests that the Coast Guard clarify the extent of the area within a facility that is covered by the TIR. API believes it is reasonable for the Coast Guard to regulate security for that part of the "facility" that could be impacted by waterborne and/or ship-to-shore activities. Therefore, API recommends that the final rule provide for a means to identify a natural or logical barrier that will indicate the extent of the Coast Guard authority over facility security.
- (c)(3)(ii) The regulations exclude a facility that supports the "production, exploration, or development of oil and natural gas ....if the facility transports ***or stores*** (emphasis added) hazardous materials that do not meet or exceed those specified in 49 CFR 172.800(b)(1) through (6)...". We recommend that "or stores" be deleted to be consistent with the intent of the Department of Transportation regulations established by the Research and Special Programs Administration (RSPA) on March 25, 2003 (68 FR 14510) for transporters of hazardous materials. We recommend that 105.105(c)(3)(ii) be revised to read as follows: "The facility transports ~~or stores~~ quantities of hazardous materials that do not meet and exceed those specified in 49 CFR 172.800(b)(1) through (6); ~~or~~ *and*" (*added*)

105.105 (c)(3) is intended to exclude small shorebases (part 126) and/or small fueling facilities (part 154) supporting "oil and natural gas production, exploration and development" facilities provided that the hazardous materials that are being transported do not exceed threshold quantities established by RSPA (49 CFR 172.800). Shorebases are land based support facilities that may provide marine and/or air transportation of cargo, stores and personnel to oil and natural gas facilities defined in 106.105 and 105.105(c)(2). Some of these facilities may store quantities of Part 154 cargo used to support oil and natural gas operations (105.105 (c)(3)(iii). Replacing "or" with "and" at the end of 105.105 (c)(3)(ii) will clarify that to be excluded from applicability both criteria must be met.

## ***Subpart B – Facility Security Requirements***

### **Section 105.200 Owner or operator**

- (b)(9) API does not support the notification of the National Response Center (NRC) for all breaches of security at a facility. Breaches of security are not adequately defined and, as such, could lead to both under reporting and over reporting. It is not clear what NRC would do with the information nor how such a notification would improve facility security. Rather, such notifications should be made to the COTP and other local law enforcement officials. API does support notification of the NRC for an actual transportation security incident.

### **Section 105.205 Facility Security Officer**

- (a)(2) & (a)(3) The qualifications for an FSO as shown in Section 105.205(b) are very detailed and are more than are needed for an FSO at many facilities that pose less risk. Thus, API questions the reasonableness of requiring an FSO for covered oil and natural gas facilities, many of which are small, remote or pose little risk. For these types of facilities, API believes the facility manager can function as the FSO as long as he/she has a strong awareness of security issues for that facility. While the TIR does allow the same person to serve as the FSO for more than one facility in the same COTP zone, product terminals and other facilities that are widely dispersed would still require companies to hire multiple security professionals.

Also, API does not support the 50-mile limitation placed on the FSO. Many facilities that are not co-located may still be managed as multiple site complexes using shared operational and administrative resources. The 50-mile limitation could prevent such facilities from sharing an FSO, even if they are similar facilities. Since Section 105.205(a)(3) allows the FSO to assign security duties to other facility personnel, API recommends that the FSO still be ultimately responsible for conducting a Facility Security Assessment (FSA) and ensuring the development and implementation of the Facility Security Plan (FSP) but assign the day-to-day security activities to local personnel.

### **Section 105.215 Security training for all other facility personnel**

- In general, API supports the training of facility personnel on facility security, the requirements for the MARSEC levels, and emergency response procedures. However, API believes it is unreasonable to expect facility personnel and contractors to be trained in recognition of dangerous substances and devices, recognition of behavioral patterns and especially techniques to circumvent security measures. Such activities should be left to other suitable facility personnel. Facilities may be responsible for basic orientation-level training.

### **Section 105.225 facility recordkeeping requirements**

- The majority of the recordkeeping requirements specified in Sections 106.230 and 105.225 are overly burdensome and unnecessary. API urges the USCG to reconsider its position and suggests these sections be modified as follows:
  - 1) API has no objection to maintaining the following records specified in the temporary interim rules for two years provided they may be kept in an electronic

format and stored at the office where such business records are normally maintained and updated. Records storage at the facility or aboard the vessel should remain optional. Such records would be accessible to the USCG, upon request:

- a) 106.230(b)(1) and 105.225(b)(1) *Training*;
  - b) 106.230(b)(2) and 105.225(b)(2) *Drills and Exercises*, provided the appropriate Security Officer determines the best practices referenced and included in these records, if any, are allowed to be segregated from the drill and exercise record.
  - c) 106.230(b)(8) and 105.225(b)(8) *Annual Audit of the Security Plan*.
- 2) API requests the following requirements be deleted or, alternatively, modified as reflected:
- a) 106.230(b)(3) and 105.225(b)(3) *Incidents and Breaches of Security*.
  - b) 106.230(b)(4) and 105.225(b)(4) *Changes in MARSEC Levels*.
  - c) 106.230(b)(5) and 105.225(b)(5) Maintenance, calibration and testing of security equipment. An alternative would be to exempt routine maintenance (preventative and otherwise), calibration and testing, but maintain the recordkeeping requirement for instances where the involved security equipment is out of service for a lengthy period of time while being repaired or awaiting receipt of replacement parts or a service technician. Also, API recommends that recording the “time” be removed from the regulation because it adds an unnecessary recordkeeping burden on the OCS personnel. Maintenance activities are often tracked by the date of completion, not time and date.
  - d) 106.230(b)(6) and 105.225(b)(6) *Security Threats*. An alternative would be to require recordkeeping when a credible threat is received relative to a specific covered facility under Parts 106 or 105, which has been verified through communication with the USCG or another DHS agency.
  - e) 106.230(b)(7) and 105.225(b)(7) *Declaration of Security (DoS)*.

The ISPS Code only addresses the recordkeeping elements specified in Sections 106.230 and 105.225 as requirements for ships (vessels). ISPS does not require such recordkeeping requirements for facilities, and API supports this differentiation. The terms *Incidents* and *Breaches of Security* are not properly defined. This could literally mean a person going through the wrong gate or accidentally following an authorized individual into a Restricted Area. API does not think the USCG meant to have such actions documented and be covered by the recordkeeping requirements.

API sees no benefit or value in keeping records of MARSEC level changes. Maintaining records for each test, calibration or maintenance process performed on security equipment is unwarranted. API would support the alternative language offered above.

The term *Security Threats* is also not defined. It is API’s position that only credible threats received relative to a specific covered facility under Parts 106 or 105 and verified through communication with the USCG or another DHS agency should require recordkeeping.

Concerning the DoS recordkeeping requirement, as stated in our separate comments on this item, API does not see the need for the DoS to be utilized at any covered oil and natural gas facility or their supporting vessels. If this requirement is unnecessarily retained, it is unrealistic to require that a covered facility should keep such records for at least 90 days after the end of its effective period.

#### Section 105.230 Maritime Security (MARSEC) Level coordination and implementation

- (b)(1) API does not believe it is the responsibility of the facility to notify a vessel that is not yet moored at the facility that the MARSEC level has changed. That should be the responsibility of the Coast Guard or the ship's agent.

#### Section 105.235 Communications

- This section describes the communications requirements for the TIR. API would like the USCG to clarify that these requirements apply to facility personnel and are not meant to cover communications involving the general public using facility communications equipment.

#### Section 105.260 Security measures for restricted areas

- (b) Designation of Restricted Areas. API urges the USCG to clarify the wording that states – “Restricted areas must include, as appropriate.” It seems contradictory to impose a requirement (i.e., “must include”) and then offer flexibility by stating “as appropriate”. API recommends the wording be changed to say “Restricted areas may include, as appropriate” since actual restricted areas will be site-specific and thus flexibility is needed.

### **Subpart C – Facility Security Assessment (FSA)**

#### Section 105.305 Facility Security Assessment (FSA) requirements

- In this section, the USCG requires a very prescriptive approach for a facility security assessment. Many petroleum facilities have already conducted security assessments using one of many other available methods. For example, API and NPRA recently published the “Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries.” This document was developed in close cooperation with the DHS and DOE’s Argonne Laboratory and included pilot testing at industry facilities. Similarly, Appendix E of *API RP 70* has an assessment methodology for exploration and production facilities. As requested earlier in these comments, API encourages the USCG to approve these SVA methodologies as alternatives to the prescriptive Section 105.305 language.

#### Section 105.310 Submission requirements

- API does not support the requirement to submit the FSA with the FSP. The FSA is a document that details the possible threats, vulnerabilities, consequences and protective measures, procedures and operations of a facility. The FSA is the basis for the development of the FSP, which is the plan of how the facility will be protected. The Maritime Transportation Security Act of 2002 does not require that assessments be provided to the Coast Guard. Section 70103 © Vessel and Facility Security Plans

requires a security plan be developed and submitted to the Secretary for approval but does not require the submittal of the security assessments.

In addition, Sections 105.210 and 105.215 require training on relevant parts of the FSP that could include security details from the FSA. API does not believe that facility personnel need to know the details of the FSA in order to be trained on security, action to take in the case of a TSI and emergency response. Therefore, API believes the security details contained in the FSA should remain with the facility and should not be required to be submitted to the COTP with the FSP.

#### **Subpart D – Facility Security Plan (FSP)**

##### **Section 105.400 General**

- (c) This section states the FSP is sensitive security information (SSI) and will be protected in accordance with 49 CFR Part 1520. However, the requirements in Part 1520 are more transportation oriented, mainly aircraft, and do not specify the protocols the COTP can use to protect the SSI. API recommends consistent guidance be developed to ensure SSI is adequately protected from disclosure to the public.

**Re: National Maritime Security Initiatives**  
**Docket: USCG-2003-14759, Part 106**

***V. Subchapter H – Maritime Security***  
***Part 106 – Outer Continental Shelf Facility Security***

***Subpart A – General***

**Section 106.105 Applicability**

- The operating conditions referenced in 106.105(a), (b) and (c) as well as the thresholds and excluded facilities specified in Section 105.105 should remain as written, adopting the clarifications and revisions relative to Section 105.105(c)(3). Additionally, API endorses the comments from the International Association of Drilling Contractors (IADC) in connection with Section 104.105 Applicability, as it relates to Mobile Offshore Drilling Units (MODUs).

We commend the USCG for establishing generally reasonable operating conditions, thresholds and exempted facilities based on risk assessments conducted pursuant to the requirements of Public Law 107-295 (MTSA) Section 70102. However, we are concerned by the comments found throughout the interim rules that state or intimate these parameters are under review for potential revisions. Several (non-exclusive) of the pertinent interim rule citations are as follows:

- 1) Part 101 and 102 Preamble, Federal Register page 29249: “As mentioned in the above *Applicability for Vessels* discussion, the 150-passenger threshold will be reviewed for the maritime community when other agencies of DHS (e.g., TSA) have completed their assessment of the national transportation system as a whole and has provided guidance on intermodel thresholds that may refine the “significant loss of life” determination for the implementation of the MTSA.”
- 2) Part 101 and 102 Preamble, Federal Register pages 29249 and 39250: “Therefore, the interim rules published today, especially the applicability sections of parts 104, 105 and 106, do not exhaust the types of vessels and facilities that may be regulated under the MTSA. We may be involved in follow-on regulations to address these adjacent facilities in the future.”
- 3) Part 101 and 102 Preamble, Federal Register page 39250: “We will continue to work with the MMS to validate this threshold as the results of the other agencies of DHS (e.g., TSA) intermodel comparisons are completed.” This cite references the 150-person threshold.

We recognize the MTSA requires the identification of vessel types and facilities that pose a high risk of being involved in a transportation security incident. Further, the MTSA defines “transportation security incident” as a security incident resulting in a significant loss of life, environmental damage, transportation system disruption or economic disruption in a particular area. API supports retaining those thresholds that have been established related to the offshore exploration and production of oil and natural gas. While API disagrees with many of the results of the N-RAT, the oil and natural gas industry and its supporting companies, are diligently working towards compliance within the framework of the Applicability sections of Parts 104, 105 and

106. These vital domestic energy concerns must have certainty and consistency in order to meet these security requirements within the time parameters mandated.

***Subpart B – Outer Continental Shelf (OCS) Facility Security Requirements***

**Section 106.220 Company or OCS facility personnel with security duties**

- In general, API supports the training of facility personnel on facility security, the requirements for the MARSEC levels, and emergency response procedures. However, API believes it is unreasonable to expect facility personnel and contractors to be trained in recognition of dangerous substances and devices, recognition of behavioral patterns and especially techniques to circumvent security measures. Such activities should be left to security personnel. The facility may be responsible for basic orientation-level training.

**Section 106.230 OCS facility recordkeeping requirements**

- The majority of the recordkeeping requirements specified in Sections 106.230 and 105.225 are overly burdensome and unnecessary. API urges the USCG to reconsider its position and suggests these sections be modified as follows:
  - 3) API has no objection to maintaining the following records specified in the temporary interim rules for two years provided they may be kept in an electronic format and stored at the office where such business records are normally maintained and updated. Records storage at the facility or aboard the vessel should remain optional. Such records would be accessible to the USCG, upon request:
    - a) 106.230(b)(1) and 105.225(b)(1) *Training*;
    - b) 106.230(b)(2) and 105.225(b)(2) *Drills and Exercises*, provided the appropriate Security Officer determines the best practices referenced and included in these records, if any, are allowed to be segregated from the drill and exercise record.
    - c) 106.230(b)(8) and 105.225(b)(8) *Annual Audit of the Security Plan*.
  - 4) API requests the following requirements be deleted or, alternatively, modified as reflected:
    - a) 106.230(b)(3) and 105.225(b)(3) *Incidents and Breaches of Security*.
    - b) 106.230(b)(4) and 105.225(b)(4) *Changes in MARSEC Levels*.
    - c) 106.230(b)(5) and 105.225(b)(5) Maintenance, calibration and testing of security equipment. An alternative would be to exempt routine maintenance (preventative and otherwise), calibration and testing, but maintain the recordkeeping requirement for instances where the involved security equipment is out of service for a lengthy period of time while being repaired or awaiting receipt of replacement parts or a service technician. Also, API recommends that recording the “time” be removed from the regulation because it adds an unnecessary recordkeeping burden on the OCS personnel. Maintenance activities are often tracked by the date of completion, not time and date.
    - d) 106.230(b)(6) and 105.225(b)(6) *Security Threats*. An alternative would be to require recordkeeping when a credible threat is received relative to a

- specific covered facility under Parts 106 or 105, which has been verified through communication with the USCG or another DHS agency.
- e) 106.230(b)(7) and 105.225(b)(7) *Declaration of Security (DoS)*.

The ISPS Code only addresses the recordkeeping elements specified in Sections 106.230 and 105.225 as requirements for ships (vessels). ISPS does not require such recordkeeping requirements for facilities, and API supports this differentiation. The terms *Incidents* and *Breaches of Security* are not properly defined. This could literally mean a person going through the wrong gate or accidentally following an authorized individual into a Restricted Area. API does not think the USCG meant to have such actions documented and be covered by the recordkeeping requirements.

API sees no benefit or value in keeping records of MARSEC level changes. Maintaining records for each test, calibration or maintenance process performed on security equipment is unwarranted. API would support the alternative language offered above.

The term *Security Threats* is also not defined. It is API's position that only credible threats received relative to a specific covered facility under Parts 106 or 105 and verified through communication with the USCG or another DHS agency should require recordkeeping.

Concerning the DoS recordkeeping requirement, as stated in our separate comments on this item, API does not see the need for the DoS to be utilized at any covered oil and natural gas facility or their supporting vessels. If this requirement is unnecessarily retained, it is unrealistic to require that a covered facility should keep such records for at least 90 days after the end of its effective period.

#### Section 106.250 Declaration of Security (DoS)

- A Declaration of Security as specified in 106.250 is not warranted between an OCS facility and vessels delivering personnel, cargo or other materials. Additionally, a DoS as specified in 104.255 and 105.245 is also not necessary between a vessel in OCS service and a facility covered by 105.105(a)(1) and 105.105(a)(3) or for a vessel operating under conditions addressed in 105.105(c) for oil and natural gas production, exploration or development operations in non-OCS waters. We urge the Coast Guard to exempt offshore supply vessels and the facilities cited herein from the DoS requirements.

API supports the guidance document concept discussed in the Preamble in Parts 101 and 102 provided the USCG revises the relevant sentence to read "For U.S. Flag Vessels or vessels and facilities engaged in or supporting oil and natural gas exploration, development or production, we intend to provide guidance to companies on when to request a DoS based on vessel operations and world threat conditions." Additionally, the guidance document should be revised to be consistent.

The vast majority of domestic inland and offshore (OCS) oil and natural gas facilities are not covered by the interim security rules. API supports the Coast Guard decision

for making this determination based on realistic risk assessments and establishing appropriate thresholds. Many offshore oil and natural gas facilities may utilize *API Recommended Practice (RP) 70, Security for Offshore Oil and Natural Gas Operations*, which was developed jointly by industry, the USCG and the Minerals Management Service. This recommended practice does not address Declarations of Security. Rather, the document focuses resources on addressing security needs, in a performance-based manner, at the point of embarkation (support bases or heliports). Moreover, the Coast Guard has already stated it may require compliance with industry standards such as *RP 70* in future rulemakings, which we generally support.

Accordingly, facility supervisory personnel, including the *RP 70* designated Facility Security Officer, will not be familiar with a DoS nor will they be trained as to its purpose and appropriate use. Offshore supply vessels (OSVs) are dedicated vessels servicing facilities engaged in production, exploration or development of oil and natural gas resources on the OCS and in other domestic waters subject to the jurisdiction of these rules. Contracted OSVs only call upon a limited and defined group of facilities. These facilities are the land-based support bases referenced in 105.105(c)(3) and oil and natural gas facilities defined in 106.105 and 105.105(c)(2).

Another consideration is that ISPS allows discretion on the part of both the Contracting Government and the vessel to determine when a DoS is necessary. The need for a DoS is generally premised upon factors such as when there is a higher risk to persons, property or the environment for reasons specific to the vessel or at the facility.

#### Section 106.255 Security Systems & Equipment Maintenance

- Section 106.255 requires that security systems and equipment be inspected, tested, calibrated and maintained according to the manufacturer's recommendation. API suggests adding language to this section to allow the OCS facility operator or owner to develop and follow other procedures, which are found to be more appropriate through experience or other means. Through experience, OCS facility personnel gain understanding in how best to maintain and test the equipment to ensure reliable operation while taking into account cost and other factors.

#### Section 106.260 Security measures for access control

- (e) MARSEC Level 1 - The regulation states that, "The OCS facility owner or operator must ensure the following security measures are implemented at the facility..." API recommends adding the words "or point of embarkation" to the sentence so that it reads "... at the facility or point of embarkation." The point of embarkation is often the primary location for controlling access to the OCS facility. Unlike the OCS facility, the point of embarkation is land-based, and therefore more resources, such as trained security personnel and local law enforcement, are available to deter unauthorized access. Thus, the owner or operator should have the flexibility to determine whether to implement security measures at the OCS facility or point of disembarkation to control access to the OCS facility.

- (f)(1) The regulation requires “increasing the frequency and detail of screening of people and personal effects embarking on the OCS Facility.” API recommends adding the sentence: “The screening may take place at the point of embarkation.”

For reasons mentioned in (e) above, the point of embarkation is often the primary location for controlling access and inspecting persons, their personal effects, and cargo that will come aboard the OCS facility. Putting the inspection point at the OCS facility puts the offshore personnel in the position of having to confront unauthorized access where there is no local, state or federal law enforcement available to support these individuals.

- (f)(3) & (g)(3) API suggests adding the wording “... while taking safety into account.” to the end of the sentence.
- (g) MARSEC Level 3 – The point of embarkation should allowed as the primary point of control onto the OCS facility for reasons mention above in (e) and (f).
- (e)(5), (f)(3), (g)(3) The regulations specify limitations on access to the OCS facility by closing or securing some access points or even limiting the OCS facility to one access point. The access points were designed to provide sufficient egress for safe evacuation during an emergency, such as fire and explosion. In fact, there are regulatory requirements for an OCS facility to have at least two means of egress from any given area. Restricting these points of egress may impact the safety of the individuals, disproportionate to the benefit of providing more security. API suggests the USCG add language allowing the owner or operator to take into account safety while assessing whether to limit the access points.

#### Section 106.275 Security measures for monitoring

- (a) Requiring the OCS owner or operator to continuously monitor the OCS facility and surrounding area is overly burdensome considering the benefit of doing so. API suggests that the word “continuously” be replaced with the word “frequent.”
- Continuous monitoring implies that all aspects of the facility and surroundings are under surveillance all of the time. OCS facilities are located in the ocean in plain view. Frequent monitoring would allow personnel to identify a vessel or aircraft in the vicinity of the OCS facility. The more important issue is what to do when a vessel is located near an OCS facility for a period of time, and then attempts an unauthorized entry or a terrorist act. Continuous monitoring places a significant burden on the OCS facilities owner or operator because increased staff levels would be necessary to keep watch not only on the facility, but also the surrounding area.

### **Subpart C – Outer Continental Shelf (OCS) Facility Security Assessment (FSA)**

#### Section 106.305 Facility Security Assessment (FSA) requirements

- In this section, the USCG requires a very prescriptive approach for a facility security assessment. Many oil and gas producing companies have already conducted assessments using one of many other available methods, including those outlined in *API RP70* and USCG NVICs 10-02 and 11-02. The API recommended practice,

which was developed at the request of USCG headquarters, and was developed jointly by representatives from the USCG, industry, and the Minerals Management Service, includes an assessment methodology that is based on USCG NVICs 10-02 and 11-02. API recommends that the USCG allow that this *API RP70* methodology be allowed as an alternative to the prescriptive Section 106.305 language that was originally developed for ships, not offshore facilities. See API comments on Section 101.510 also.

**Subpart D – Outer Continental Shelf (OCS) Facility Security Plan (FSP)**

**Section 106.415 Amendment and Audit**

- (b) The USCG requires that an audit of the FSP be conducted annually. API recommends that this be changed to every two years to be consistent with USCG audit requirements for Emergency Response Plans. This would allow operators to conduct these audits at the same time.